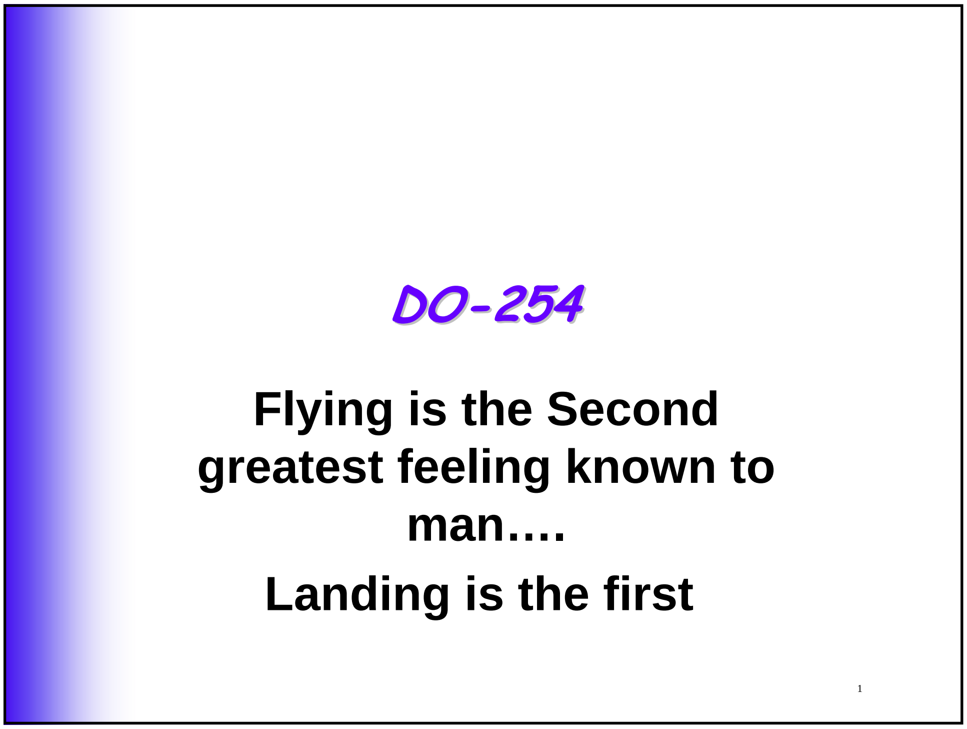
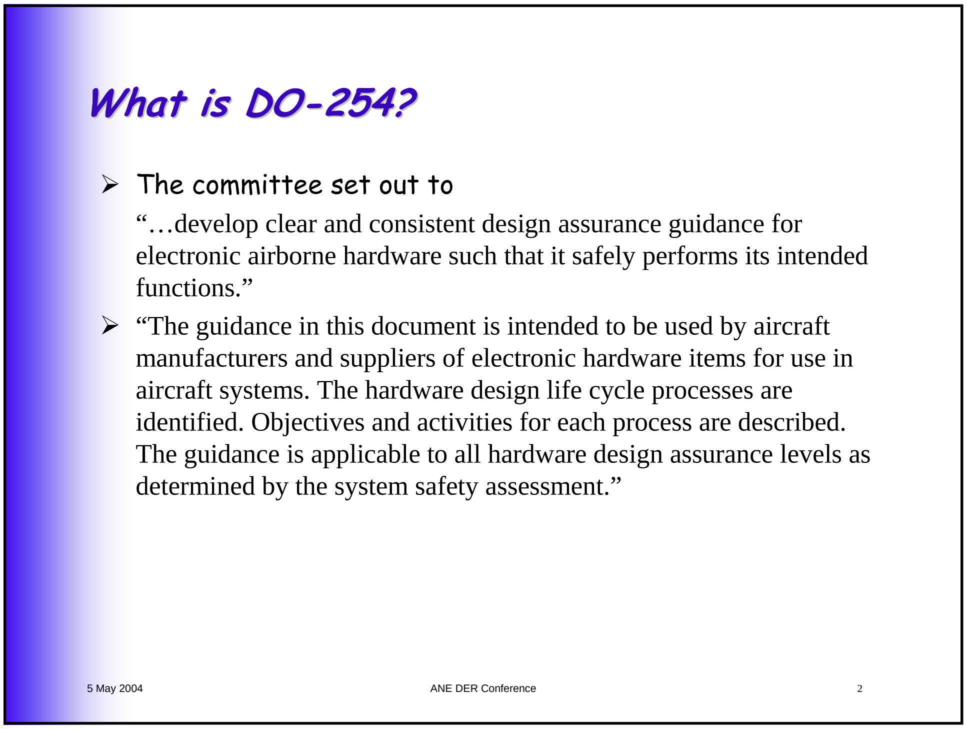


DO-254

Flying is the Second greatest feeling known to man….

Landing is the first

1

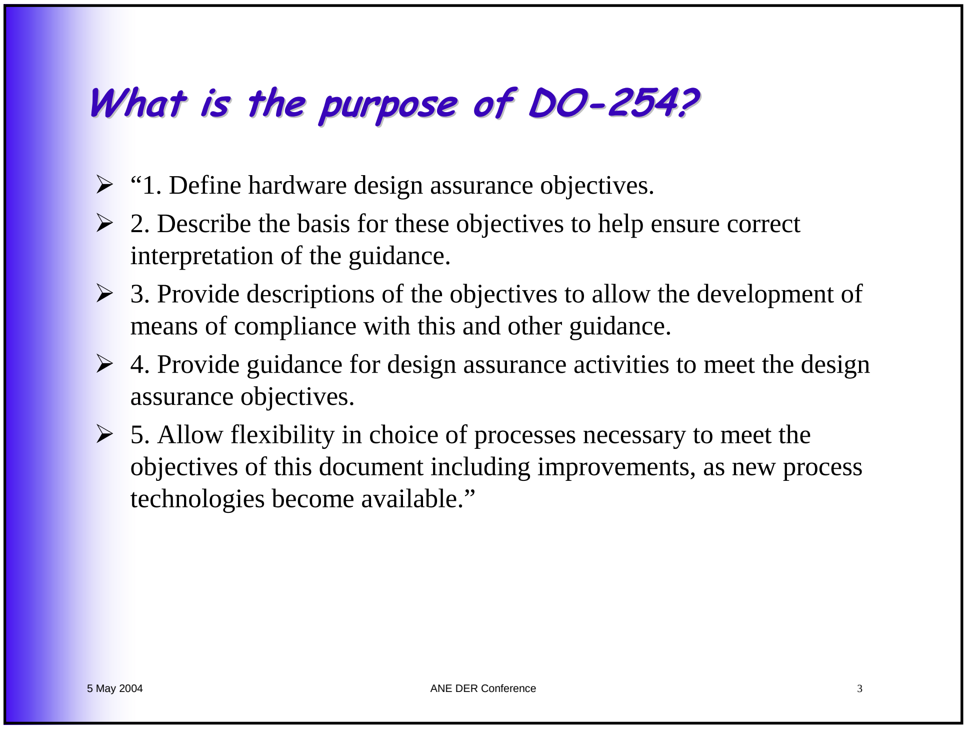


What is DO-254?

- The committee set out to

  "…develop clear and consistent design assurance guidance for electronic airborne hardware such that it safely performs its intended functions."
- "The guidance in this document is intended to be used by aircraft manufacturers and suppliers of electronic hardware items for use in aircraft systems. The hardware design life cycle processes are identified. Objectives and activities for each process are described. The guidance is applicable to all hardware design assurance levels as determined by the system safety assessment."

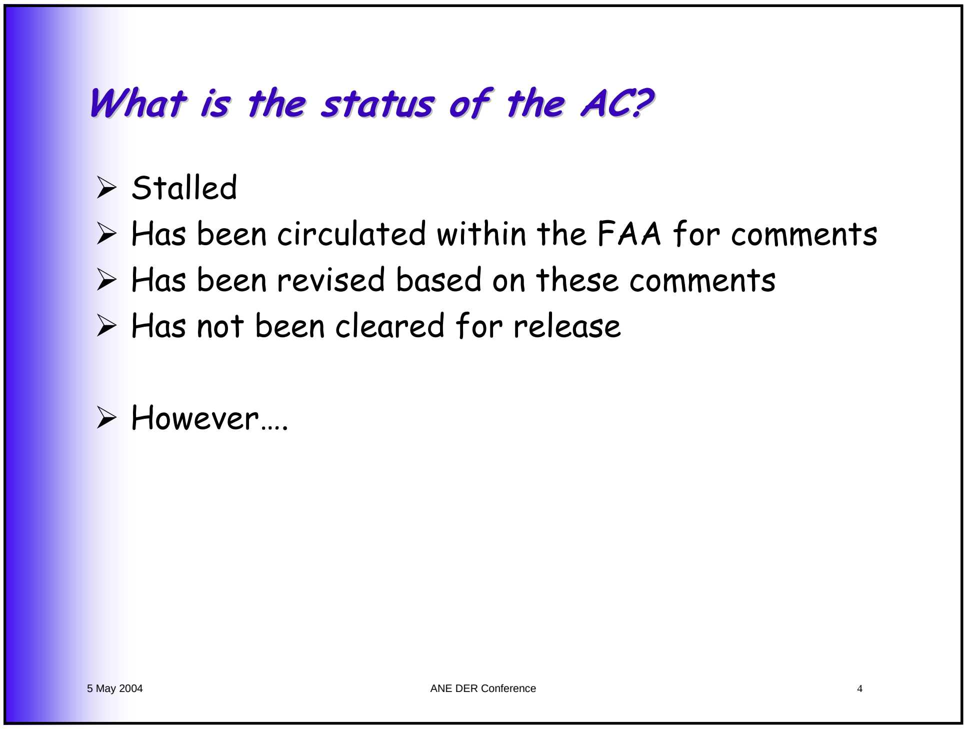
5 May 2004 ANE DER Conference 2



What is the purpose of DO-254?

- “1. Define hardware design assurance objectives.
- 2. Describe the basis for these objectives to help ensure correct interpretation of the guidance.
- 3. Provide descriptions of the objectives to allow the development of means of compliance with this and other guidance.
- 4. Provide guidance for design assurance activities to meet the design assurance objectives.
- 5. Allow flexibility in choice of processes necessary to meet the objectives of this document including improvements, as new process technologies become available.”

5 May 2004 ANE DER Conference 3

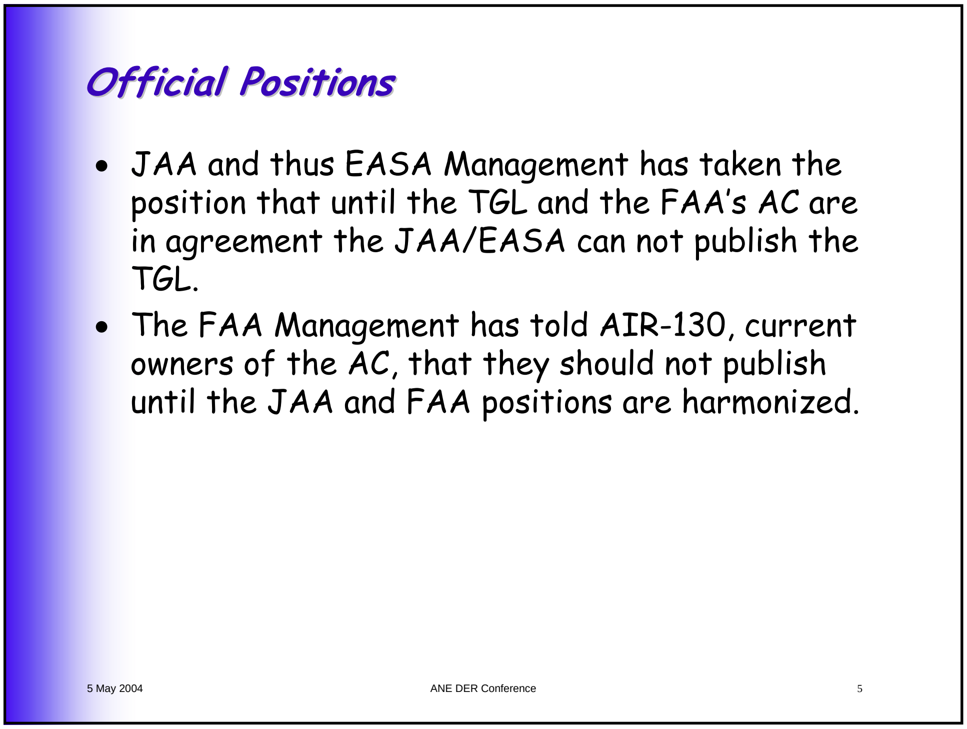


What is the status of the AC?

- Stalled
- Has been circulated within the FAA for comments
- Has been revised based on these comments
- Has not been cleared for release

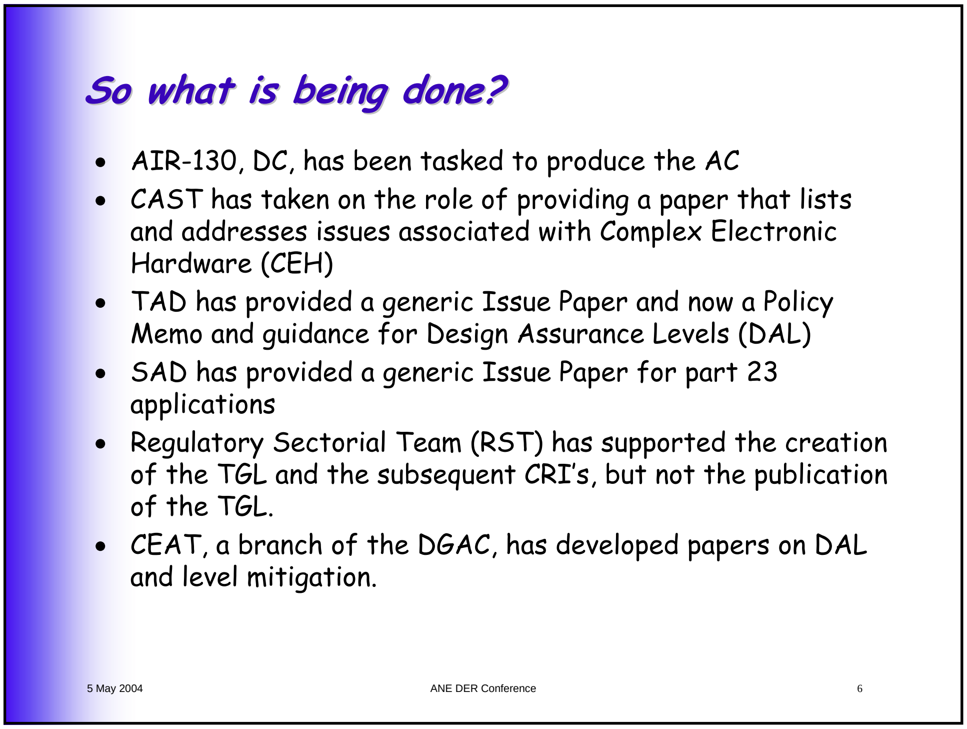
- However….

5 May 2004 ANE DER Conference 4



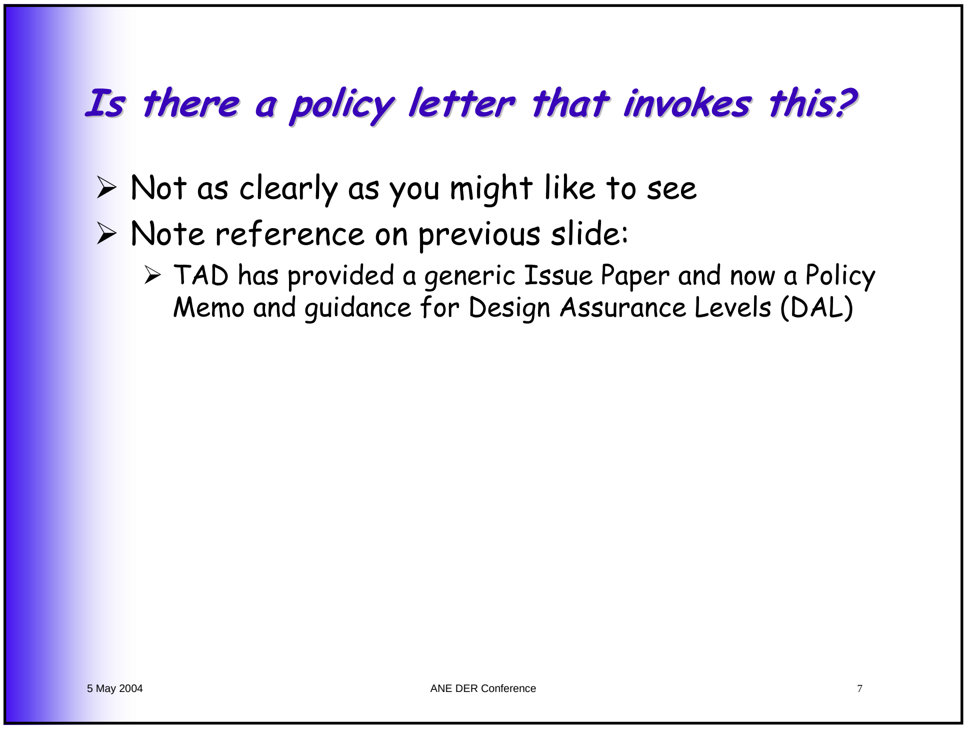
Official Positions

- JAA and thus EASA Management has taken the position that until the TGL and the FAA's AC are in agreement the JAA/EASA can not publish the TGL.
- The FAA Management has told AIR-130, current owners of the AC, that they should not publish until the JAA and FAA positions are harmonized.



So what is being done?

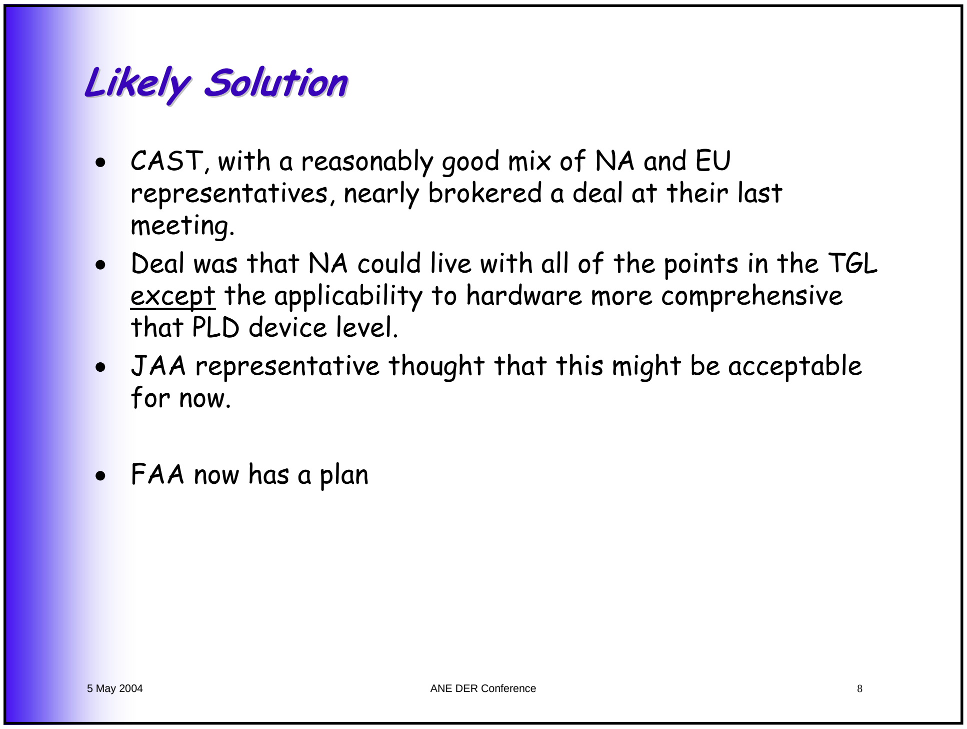
- AIR-130, DC, has been tasked to produce the AC
- CAST has taken on the role of providing a paper that lists and addresses issues associated with Complex Electronic Hardware (CEH)
- TAD has provided a generic Issue Paper and now a Policy Memo and guidance for Design Assurance Levels (DAL)
- SAD has provided a generic Issue Paper for part 23 applications
- Regulatory Sectorial Team (RST) has supported the creation of the TGL and the subsequent CRI's, but not the publication of the TGL.
- CEAT, a branch of the DGAC, has developed papers on DAL and level mitigation.



Is there a policy letter that invokes this?

- Not as clearly as you might like to see
- Note reference on previous slide:
  - TAD has provided a generic Issue Paper and now a Policy Memo and guidance for Design Assurance Levels (DAL)

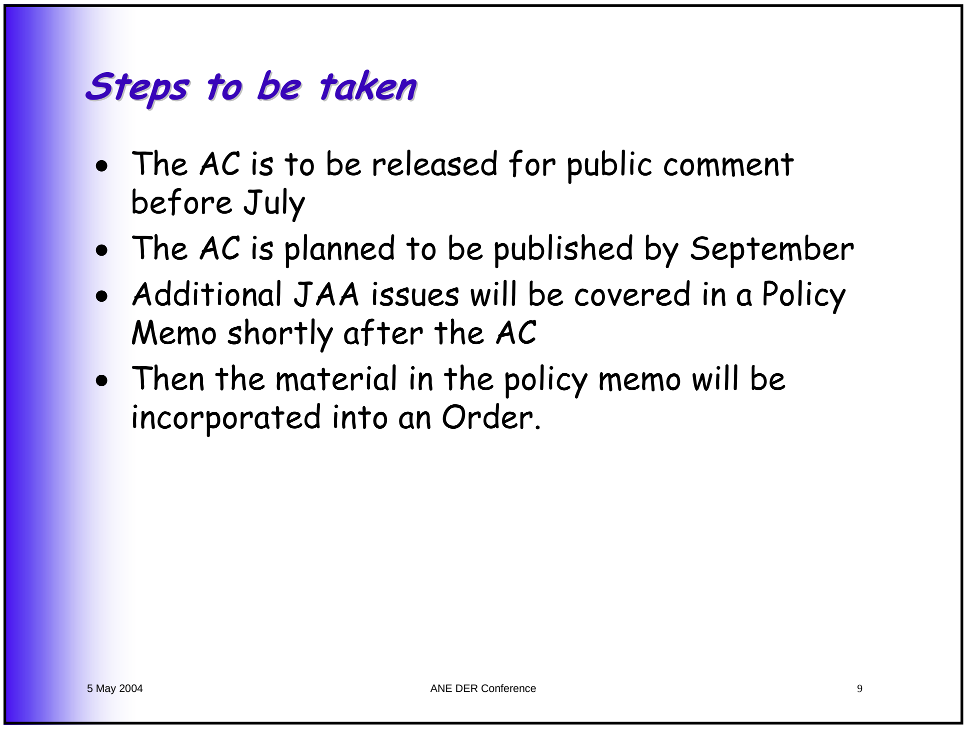
5 May 2004 ANE DER Conference 7



Likely Solution

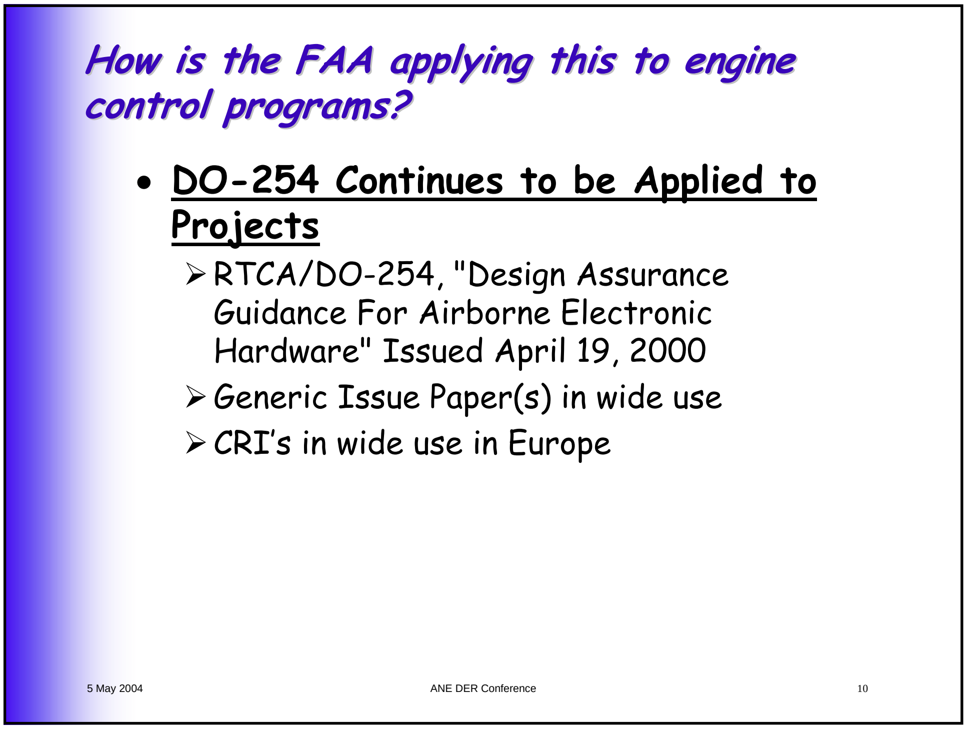
- CAST, with a reasonably good mix of NA and EU representatives, nearly brokered a deal at their last meeting.
- Deal was that NA could live with all of the points in the TGL <u>except</u> the applicability to hardware more comprehensive that PLD device level.
- JAA representative thought that this might be acceptable for now.
- FAA now has a plan

5 May 2004 ANE DER Conference 8



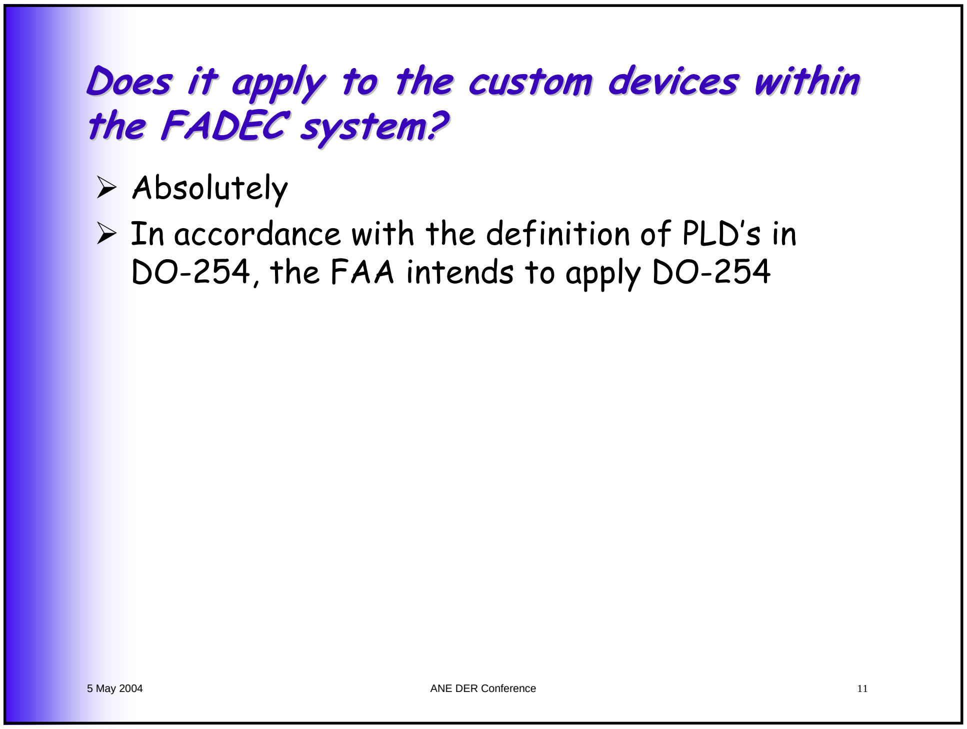
Steps to be taken

- The AC is to be released for public comment before July
- The AC is planned to be published by September
- Additional JAA issues will be covered in a Policy Memo shortly after the AC
- Then the material in the policy memo will be incorporated into an Order.



How is the FAA applying this to engine control programs?

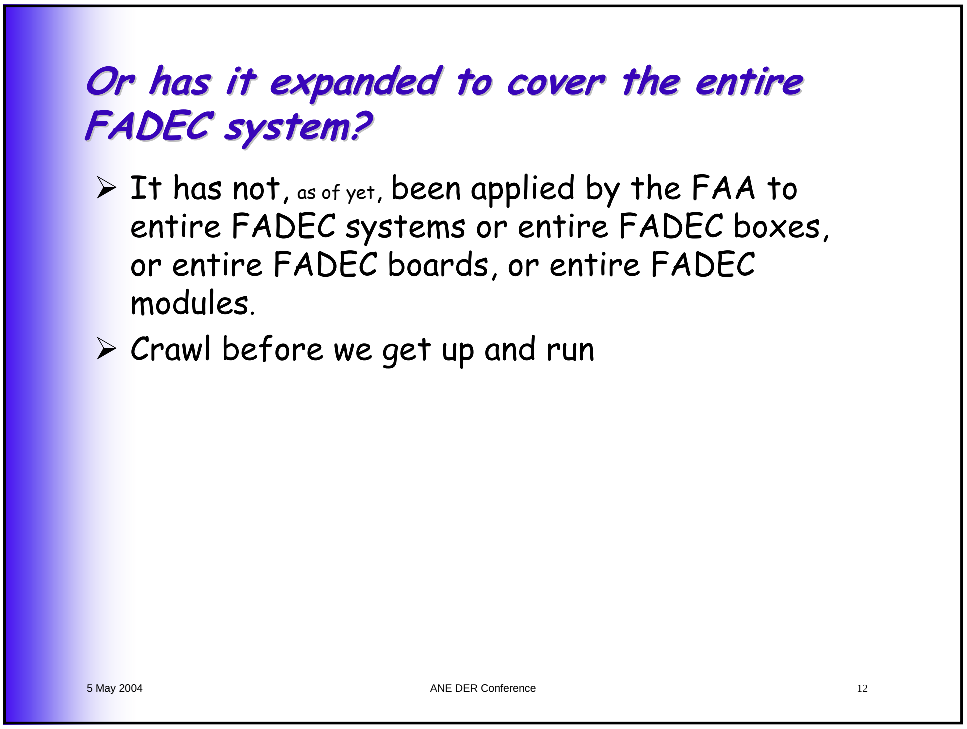
- **DO-254 Continues to be Applied to Projects**
  - ➢ RTCA/DO-254, "Design Assurance Guidance For Airborne Electronic Hardware" Issued April 19, 2000
  - ➢ Generic Issue Paper(s) in wide use
  - ➢ CRI’s in wide use in Europe



Does it apply to the custom devices within the FADEC system?

- Absolutely
- In accordance with the definition of PLD's in DO-254, the FAA intends to apply DO-254

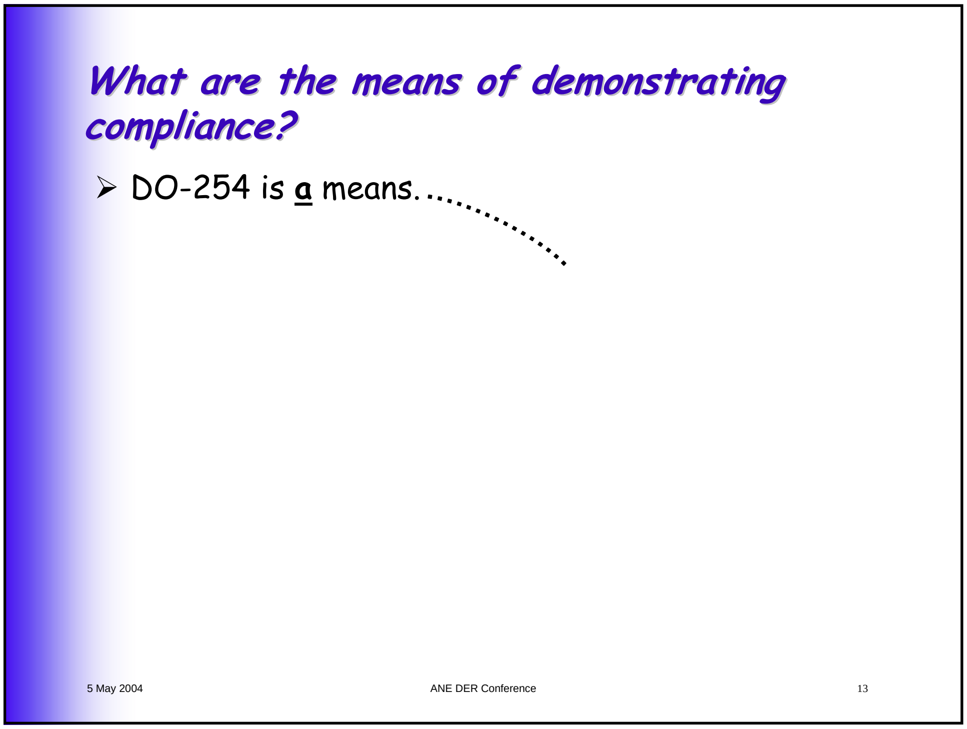
5 May 2004 ANE DER Conference 11



Or has it expanded to cover the entire FADEC system?

- It has not, as of yet, been applied by the FAA to entire FADEC systems or entire FADEC boxes, or entire FADEC boards, or entire FADEC modules.
- Crawl before we get up and run

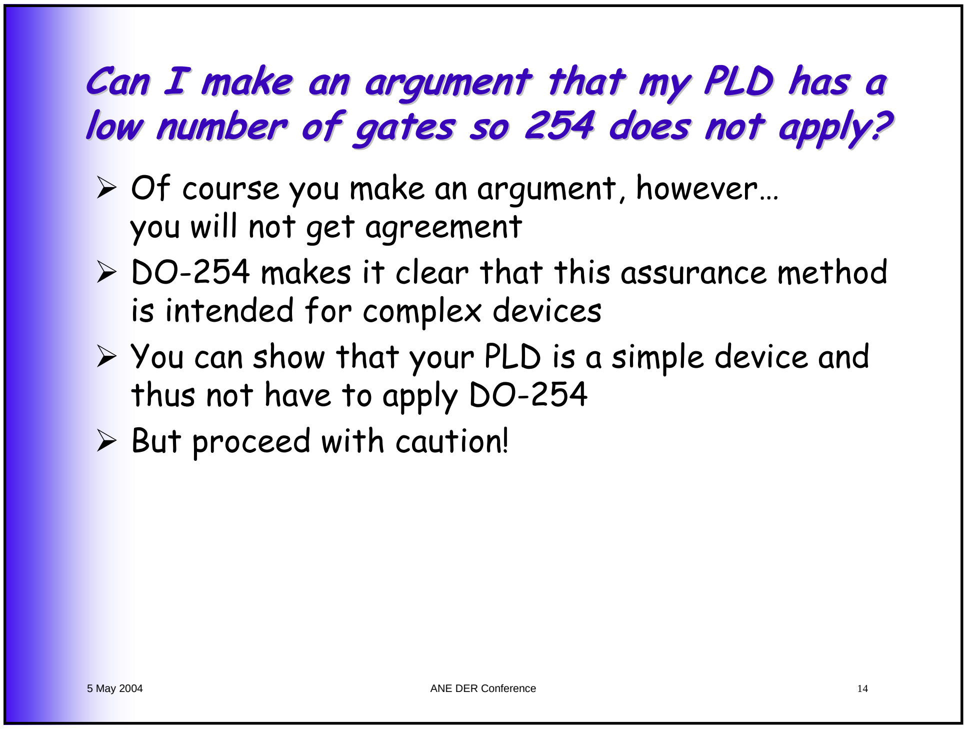
5 May 2004 ANE DER Conference 12



What are the means of demonstrating compliance?

- DO-254 is a means…

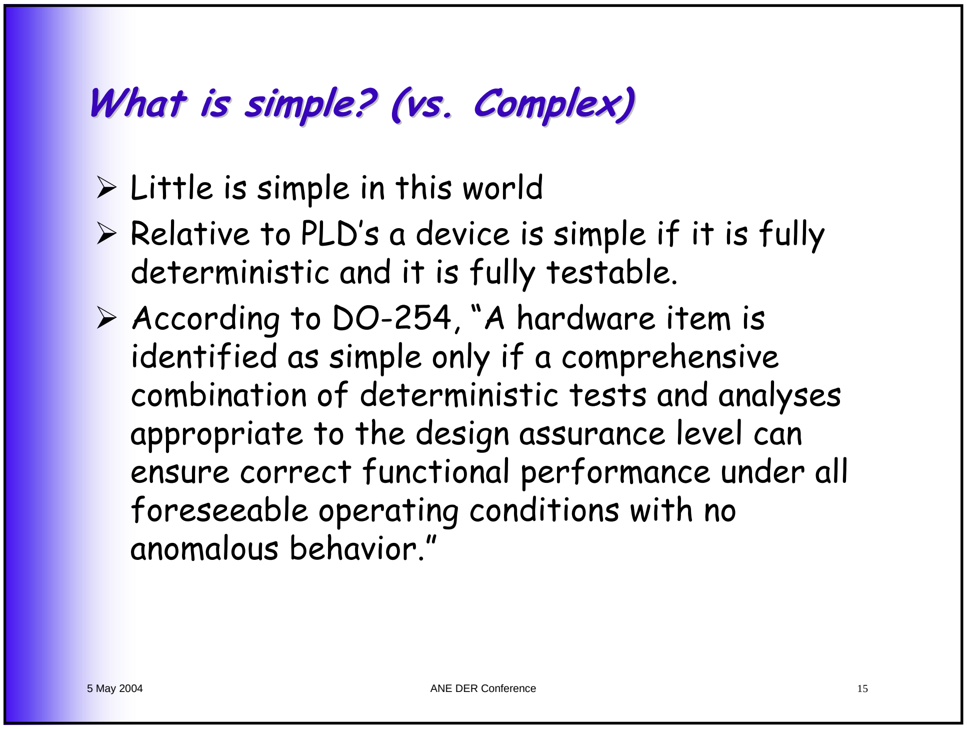
5 May 2004 ANE DER Conference 13



Can I make an argument that my PLD has a low number of gates so 254 does not apply?

- Of course you make an argument, however…
  you will not get agreement
- DO-254 makes it clear that this assurance method is intended for complex devices
- You can show that your PLD is a simple device and thus not have to apply DO-254
- But proceed with caution!

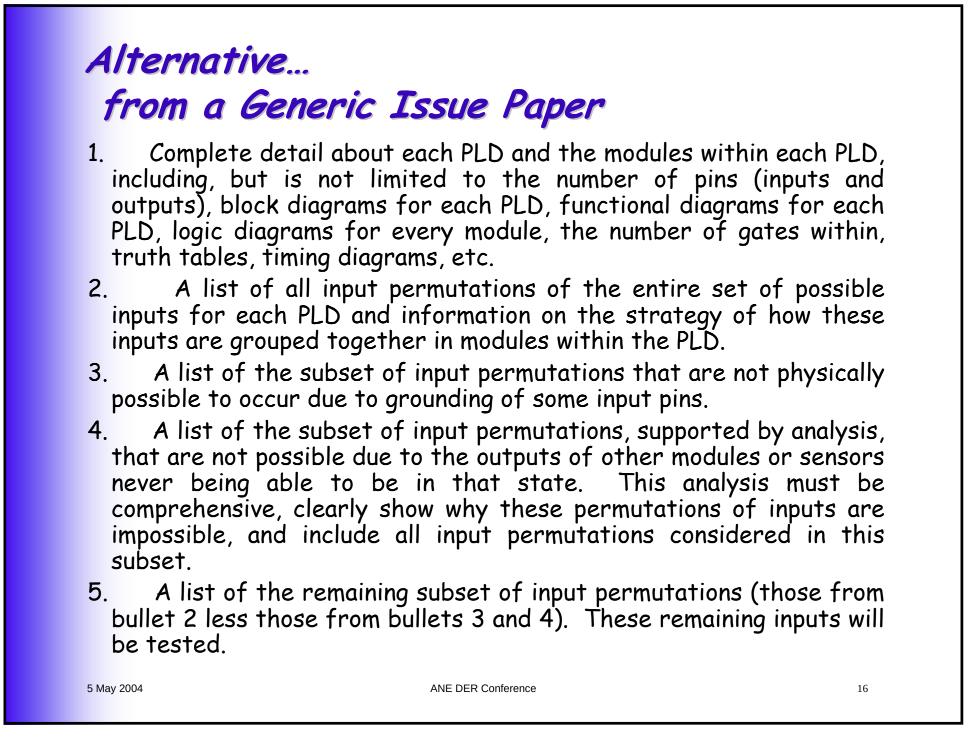
5 May 2004 ANE DER Conference 14



What is simple? (vs. Complex)

- Little is simple in this world
- Relative to PLD’s a device is simple if it is fully deterministic and it is fully testable.
- According to DO-254, “A hardware item is identified as simple only if a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior.”

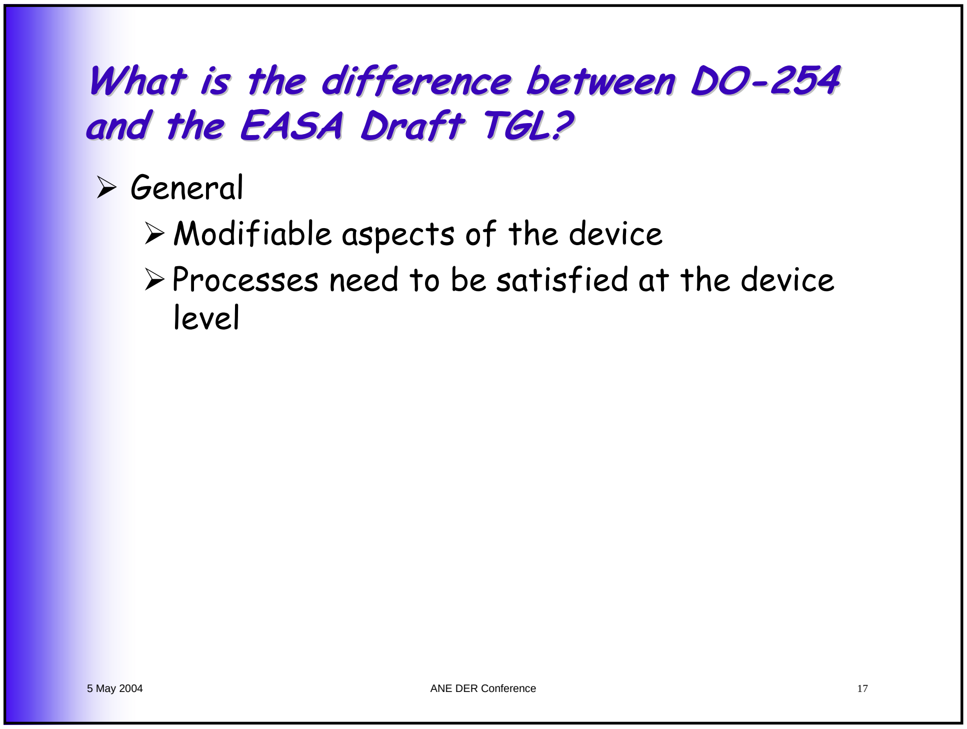
5 May 2004 ANE DER Conference 15



Alternative… from a Generic Issue Paper

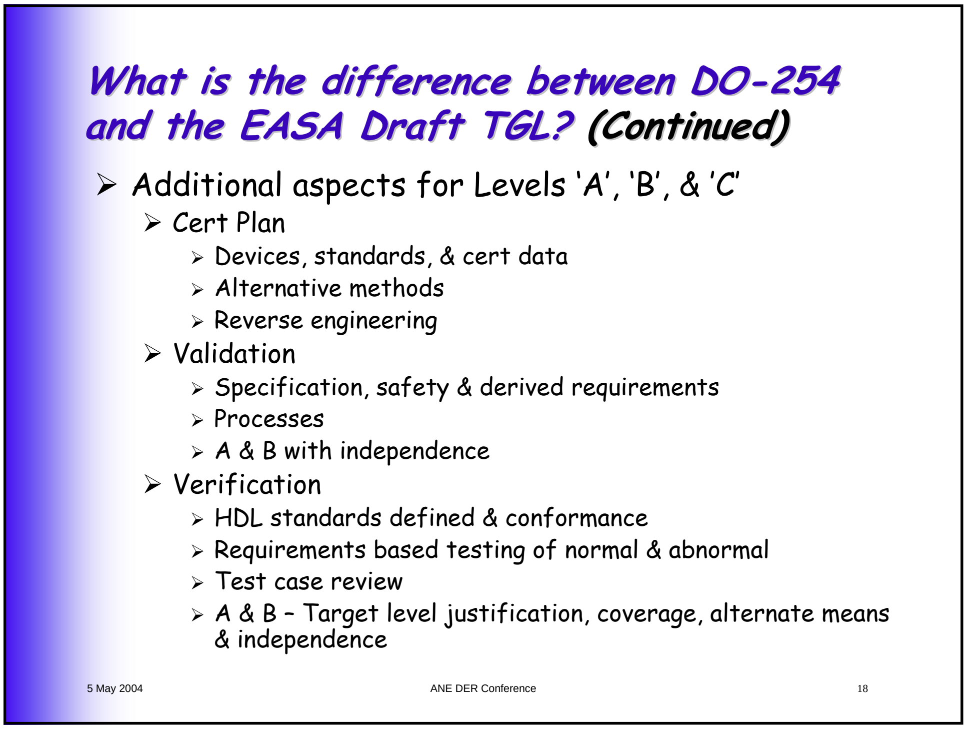
1. Complete detail about each PLD and the modules within each PLD, including, but is not limited to the number of pins (inputs and outputs), block diagrams for each PLD, functional diagrams for each PLD, logic diagrams for every module, the number of gates within, truth tables, timing diagrams, etc.
2. A list of all input permutations of the entire set of possible inputs for each PLD and information on the strategy of how these inputs are grouped together in modules within the PLD.
3. A list of the subset of input permutations that are not physically possible to occur due to grounding of some input pins.
4. A list of the subset of input permutations, supported by analysis, that are not possible due to the outputs of other modules or sensors never being able to be in that state. This analysis must be comprehensive, clearly show why these permutations of inputs are impossible, and include all input permutations considered in this subset.
5. A list of the remaining subset of input permutations (those from bullet 2 less those from bullets 3 and 4). These remaining inputs will be tested.

5 May 2004 ANE DER Conference 16



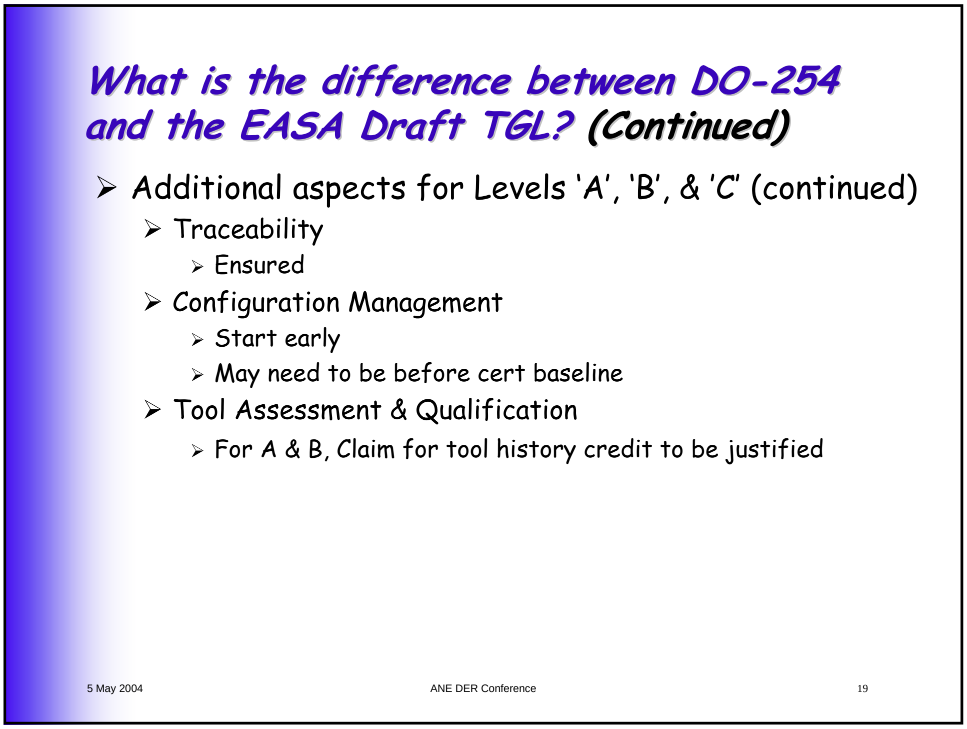
What is the difference between DO-254 and the EASA Draft TGL?

- General
  - Modifiable aspects of the device
  - Processes need to be satisfied at the device level



What is the difference between DO-254 and the EASA Draft TGL? (Continued)

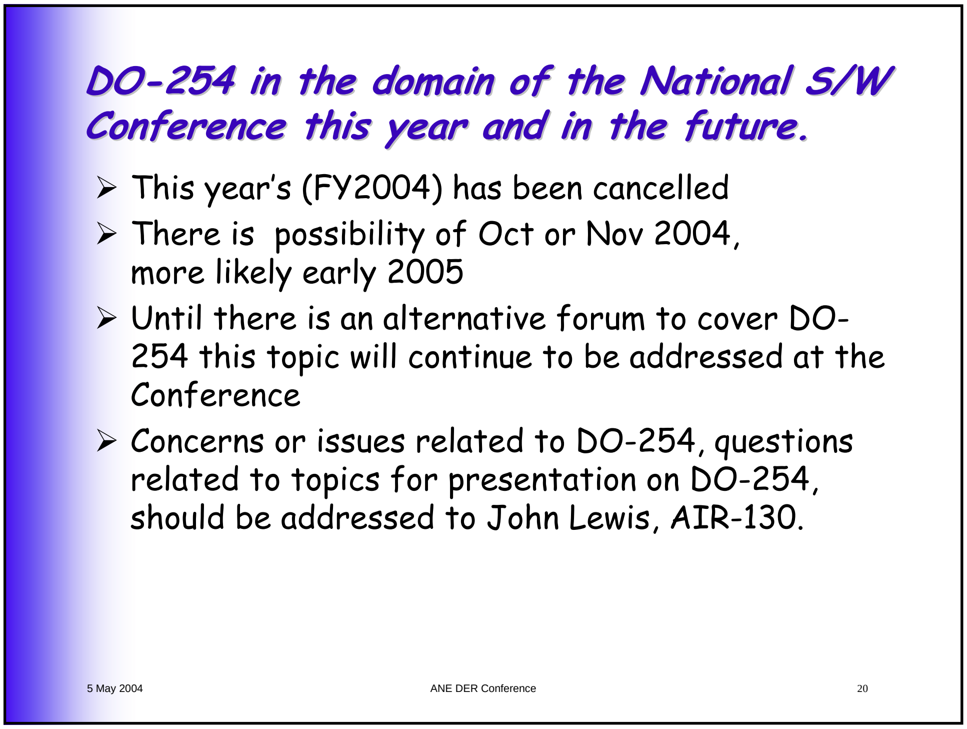
- Additional aspects for Levels 'A', 'B', & 'C'
  - Cert Plan
    - Devices, standards, & cert data
    - Alternative methods
    - Reverse engineering
  - Validation
    - Specification, safety & derived requirements
    - Processes
    - A & B with independence
  - Verification
    - HDL standards defined & conformance
    - Requirements based testing of normal & abnormal
    - Test case review
    - A & B – Target level justification, coverage, alternate means & independence



What is the difference between DO-254 and the EASA Draft TGL? *(Continued)*

- Additional aspects for Levels 'A', 'B', & 'C' (continued)
  - Traceability
    - Ensured
  - Configuration Management
    - Start early
    - May need to be before cert baseline
  - Tool Assessment & Qualification
    - For A & B, Claim for tool history credit to be justified

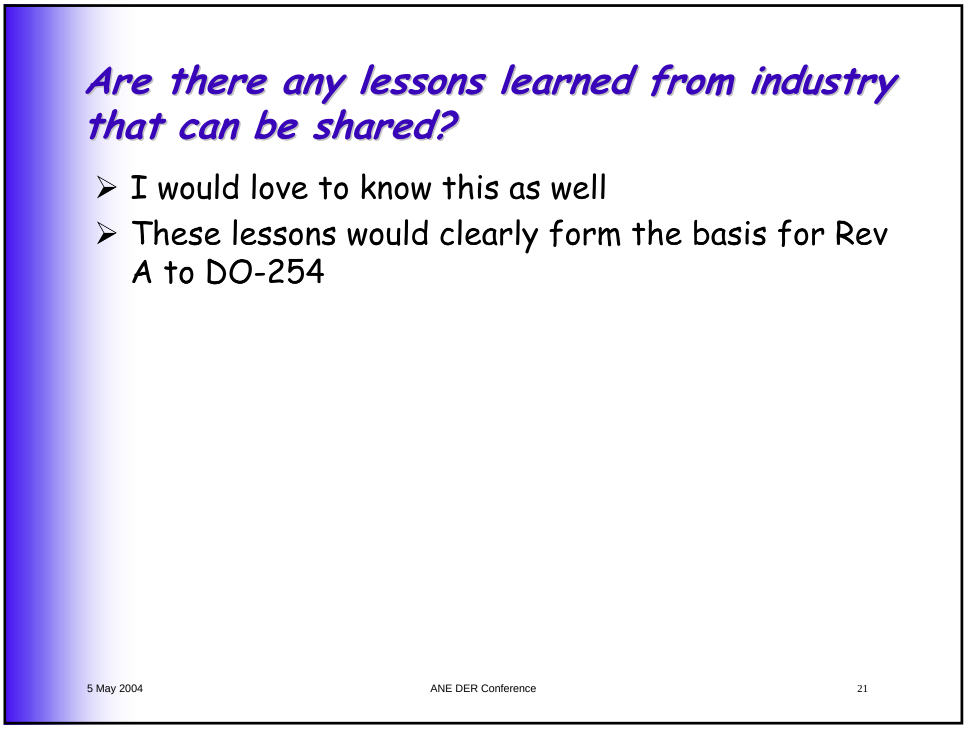
5 May 2004 ANE DER Conference 19



DO-254 in the domain of the National S/W Conference this year and in the future.

- This year's (FY2004) has been cancelled
- There is possibility of Oct or Nov 2004, more likely early 2005
- Until there is an alternative forum to cover DO-254 this topic will continue to be addressed at the Conference
- Concerns or issues related to DO-254, questions related to topics for presentation on DO-254, should be addressed to John Lewis, AIR-130.

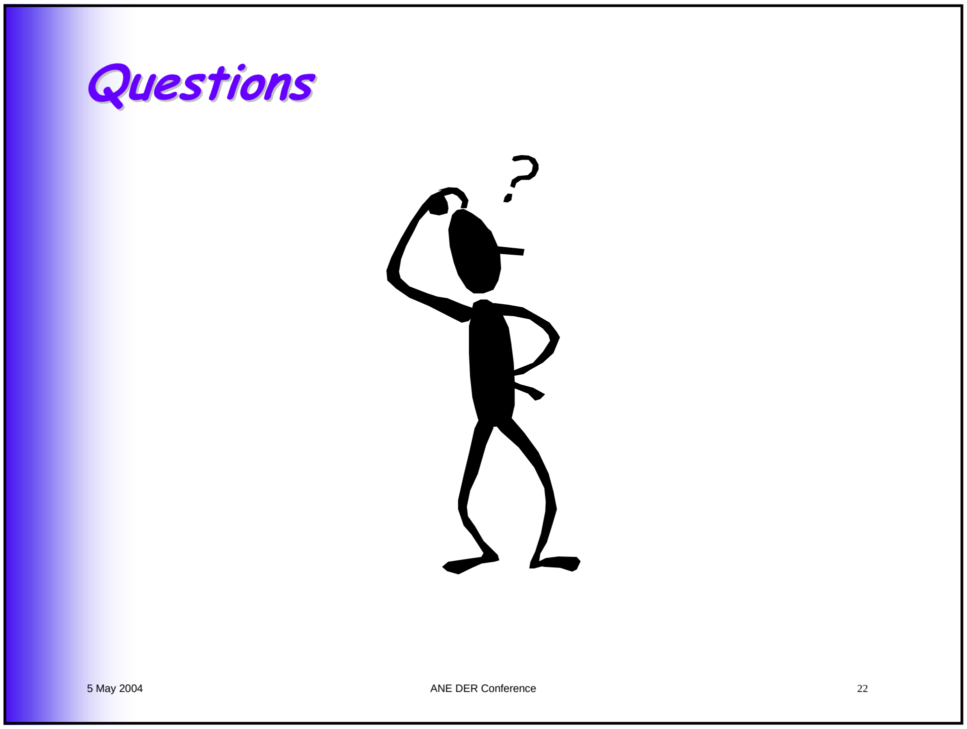
5 May 2004 ANE DER Conference 20



Are there any lessons learned from industry that can be shared?

- I would love to know this as well
- These lessons would clearly form the basis for Rev A to DO-254

5 May 2004 ANE DER Conference 21



Questions

5 May 2004 ANE DER Conference 22